End-to-End Application Security: Feasibility, Affordability, and Common Misconceptions

Slava Muchnick, EE Ltd

24/10/2014

We're EE – the most advanced digital communications company in the UK

We have the UK's biggest and fastest network, and we serve 28 million customers. For millions of people and businesses, EE is redefining what it means to be truly connected.

We have 15,000 employees and 600 stores across the country.

Our vision:

To enable our customers to make the most of their entire digital lives

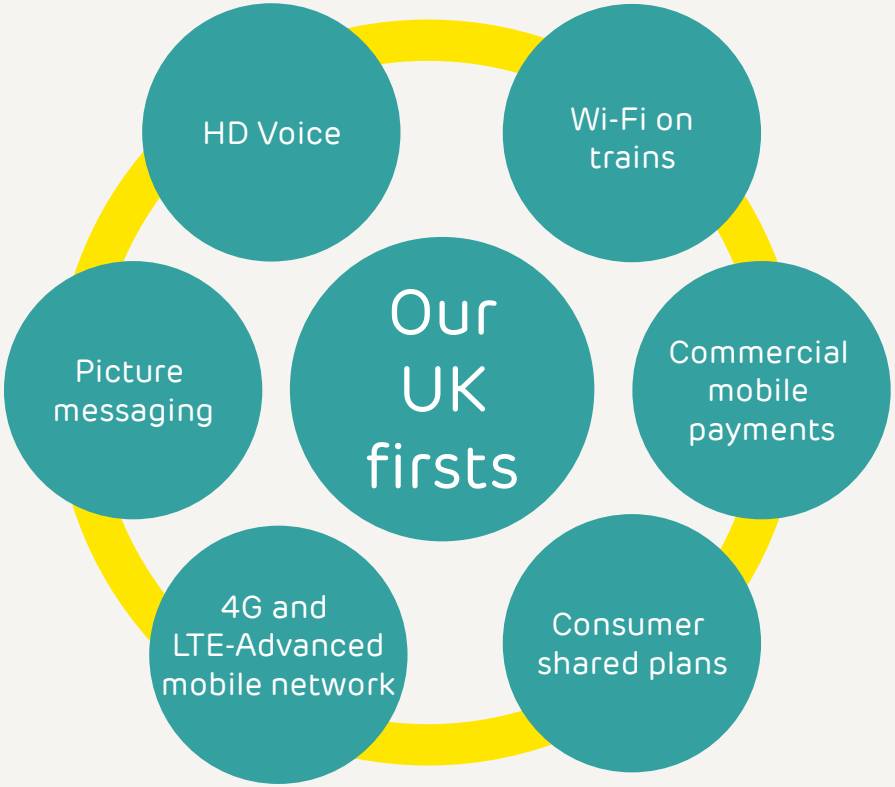
A brief history of EE

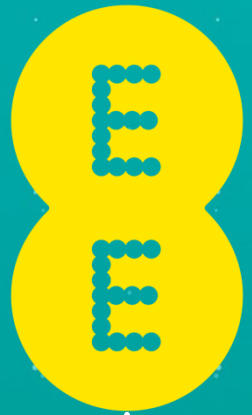
EE was formed in 2010 following the merger of Orange and T-Mobile in the UK.

T-Mobile began as Mercury one2one, founded in Borehamwood in the early 90s. It rebranded as one2one before purchase by Deutsche Telekom in 1999 and rebranded as T-Mobile.

Orange was founded in Bristol and in 1996 became the youngest ever company to enter the FTSE 100. It was acquired by France Telecom in 2000, and bought Wanadoo to add fixed broadband services alongside the mobile offering.

We have invested more than £15 billion building Britain's biggest and best mobile network.





Consumer
SME
Corporate

Consumer
SME

Consumer
SME

Fibre
ADSL

The Application Security function of EE

A dedicated AS team was established almost 10 years ago

The initial remit covered CRM systems of what used to be T-Mobile UK

Subsequently extended to cover all PCI-relevant systems of T-Mobile UK; PCI DSS certification was achieved in 2010

The current remit covers the development work on all qualifying EE systems (the list of which is defined on the basis of principles approved by Governance)

The majority of Security Analysts are based at two offshore sites for cost reasons but are selected and managed by EE – offshoring, not outsourcing

The cost of providing AS support to development projects is charged to the projects, so it needs to be budgeted for – AS Manager estimates the effort on the basis of initial project documentation

What is Application Security?

Application Security is an IT discipline dealing with the security and regulatory compliance aspects of IT systems that are specific to the application layer

Logically related matters include:

- policies and standards (external and internal)
- processes and practices
- skills according to the job role
- specialist tools

According to ISO/IEC 27034:

Application security is a process performed to apply controls and measurements to an organization's applications in order to manage the risk of using them

Current trends in the Application Security space

Attackers have changed their focus to the application layer

Realisation that application security threats require a different approach than network threats

Growing appreciation of the root causes of application vulnerabilities:

- weak processes or practices
- inadequate skills
- incomplete supporting technology

Application Security initiatives are producing measurable results

Many sectors already require secure applications, eg:

- PCI DSS is enforced for systems working with payment cards
- Federal Trade Commission has officially adopted OWASP Top 10

How is Application Security generally done?

A naive view:

Application Security can be addressed by performing “security testing” prior to deployment and then patching the code to fix the issues detected

The reality:

- Retrofitting AS to a system developed without AS in mind is not a practical option: too late, too expensive, too little can be done
- Some vulnerabilities and non-compliances can only be eliminated by adjusting the design or even the business requirements – expensive if missed at early stages
- Some AS threats are more reliably and more efficiently mitigated in the design than in the code
- Therefore, ensuring security and compliance requires undertaking review and assessment activities at all stages of the development lifecycle: an end-to-end AS process

Secure Development Lifecycle: the key points for PMs

The AS team needs to be engaged as soon as an idea for a development project has been conceived. Failure to do this is likely to impact the delivery timeline; if in doubt, engage the AS team.

Business requirements, specifications and designs have to be written down and submitted to the AS team for review. Failure to do this will dramatically inflate the cost of fixing any security issues; gamble at your peril.

Code in development has to be made available for weekly scanning. This will guarantee an early notice of any security issues in the code, leaving plenty of time for the development team to fix them.

The integration (end-to-end) testing environment has to be made available to the AS team and appropriate accounts created in it, so that final Security Audit could be performed.

No new security defects of severity Serious+ to be deployed into production. (An exemption mechanism exists: business is the ultimate decision maker.)

Cost, time and benefits

A naive view:

Application Security is an expensive activity performed for the sake of compliance; it often delays the delivery of projects and does not produce any tangible benefits

The reality:

- AS work is performed primarily to protect corporate assets and customer data entrusted to the company. Compliance is a distant second reason.
- The cost of all AS work done company-wide over several years is insignificant compared to the typical cost (direct and indirect) of a major security incident.
- When the engagement process is followed, there is usually no impact on delivery timelines. What causes delays is engaging the AS team too late.
- AS activities produce multiple artefacts that provide objective evidence of the degree of assurance achieved and of the issues still outstanding.

Delivering AS work at an affordable cost

Do not attempt to work on everything: define a scope that covers the essentials

Do not attempt to do everything: concentrate on realistic threats and aim to provide sensible mitigation

Use automation where possible (though always in combination with skilled manual work: trusting a robot to do all of your AS is asking for trouble)

Do the bulk of the manual work offshore: the nature of AS activities allows this if you do it correctly

Be clever with accounting: end-to-end AS often detects security issues early in the process, which eliminates expensive re-working and hence reduces the overall development effort; this saving offsets some of the cost of AS

Defining the scope of involvement

Regulation-driven criteria:

- Solutions involving payment card details (to ensure compliance to PCI DSS)
- Solutions involving customer data (to ensure compliance to the Data Protection Act)

Technology-driven criteria:

- Web applications
- Web services – exposing or consuming
- Mobile apps
- …

Why offshoring rather than outsourcing?

Protecting our secrets

- Able to select AS Analysts; know who of them has had access to what secrets
- The number of people who have ever worked for the AS team is kept low

Ensuring a high quality of AS deliverables

- Validating a piece of AS work would typically require doing it all over again and comparing the results

Complexity of interfaces to other development-related activities

- End-to-end AS activities permeate the whole development lifecycle
- Third parties are often involved: development/SaaS partners, testers etc

Other participants of the SDL do not always deliver to plan

- Can be creative with the AS Analysts' assignments when pre-requisites for their planned work are not ready

Other responsibilities of the Application Security team

Own and maintain the AS process integrated into the Development Lifecycle

Own and maintain EE General Application Security Requirements

Provide input into EE security policies, standards and best practices

Maintain and configure the tools used for automating some of the AS work

Provide advice and guidance to development teams in performing AS analysis and threat modelling for business requirements and technical designs

Provide consultancy services to business owners of in-house systems and to development teams in finding compromise solutions that meet the needs of the business without creating unacceptable security risks

Educate EE employees in AS matters according to their respective job roles

Relevant standards and requirements

PCI DSS (if payment cards are involved) – but it protects primarily card issuers and hence is only a baseline as far as protecting EE is concerned

Data Protection Act (if personal data is involved) – but anonymous customer data and sensitive business information also have to be protected

OWASP recommendations – cross-referenced by PCI DSS but important in their own right

In-house Application Security Requirements: a set of generic requirements applicable to all custom development done by, and for, EE; it forms part of the Security Schedule attached to all contracts with development partners and SaaS suppliers

Platform-specific in-house requirements, such as Security Requirements to Web Services